Pengembangan Prototipe Key Custodian Berbasis Server dengan Mekanisme Otorisasi Berbasis Perangkat Mobile = Prototype Development of Server-based Key Custodian with Mobile-based Authorization Mechanism

Prissy Azzahra Ratnadwita, author

Abstrak

Tanda tangan digital kini seringkali digunakan untuk melakukan verifikasi dokumen. Penyelenggaraan tanda tangan digital berkaitan erat dengan pasangan kunci, dimana private key dirahasiakan dan public key dapat disebarluaskan. Private key umumnya dikelola pada key custodian, yang bertanggung jawab atas penaganan encryption key yang dimiliki pengguna. Dalam menggunakan pasangan kunci untuk penandatanganan digital, terdapat 6 tujuan yang harus dipenuhi dalam penerapannya, yaitu authentication, integrity, confidentiality, non-repudiation, availability, dan access controls. Untuk memenuhi mekanisme otorisasi, dibutuhkan verifikasi identitas dari pemilik pasangan kunci, yang diterapkan menggunakan Three Factor Authentication (3FA). Dalam penelitian ini akan dirancang prototipe penerapan key custodian berbasis server dengan mekanisme otorisasi menggunakan modul biometrik pada perangkat mobile Android untuk memenuhi aspek ”something you are” dengan tujuan untuk memverifikasi identitas pemilik pasangan kunci. Penerapan key custodian pada server diimplementasikan menggunakan framework Django dengan memanfaatkan library PyCryptodome, dan berkomunikasi dengan perangkat mobile menggunakan JSON. Hasil dari implementasi ini masih memiliki celah keamanan, khususnya dalam aspek confidentiality dan integrity karena masih bergantung pada mekanisme pemanfaatan modul biometrik pada platform Android.
.....
Digital signatures are now often used to verify documents. The implementation of digital signatures is closely related to key pairs, where the private key is kept secret and the public key can be published. The private key is managed using a key custodian, which is responsible for handling users’ encryption keys. In the usage of key pairs for digital signatures, there are 6 objectives that must be met in its implementation, namely authentication, integrity, confidentiality, non-repudiation, availability, and access control. To fulfill the authentication aspect, identity verification of the owner of the key pair is required, which can be implemented using Three Factor Authentication (3FA). In this research, a prototype of server-based key custodian will be designed with an authorization mechanism using the biometric module on an Android device to fulfill the aspect of ”something you are” with the aim of verifying the identity of the key pair owner. The server-based key custodian is implemented using Django framework with the PyCryptodome library. The server communicates with mobile devices using JSON. The results of this implementation still have issues regarding security, especially for the aspects of confidentiality and integrity due to the limitations of biometric modules on the Android platform.